IN THE CLAIMS:

1. (Currently Amended) A user recognition system to identify a user and enable access to instruments associated with at least one implanted medical device, the system comprising:

an implanted medical device in a patient;

~~a memory associated with the implanted medical device storing coded data representative of biometric traits of authorized users to be granted access to a data communications mode of the instrument;~~

an instrument in data communications with the implanted medical device;

a memory associated with the implanted medical device storing coded data representative of biometric traits of authorized users to be granted access to the data communications of the instrument;

a sensor unit positioned along the instrument for generating biometric traits of the user; and

an analyzer unit determining whether a potential user is authorized to have access to the data communications of the instrument, wherein, in response to the potential user not being authorized to have access, the analyzer unit determines whether the potential user is requesting access associated with an override function and, in response to the access request being associated with the overdrive function, granting a level of access associated with a predetermined authorization level.

2. (Original) The system of claim 1 wherein said implanted medical device includes one of a pacer, a defibrillator, a drug delivery device and a neural implant.

3. (Original) The system of claim 1 wherein said instrument includes one of a programmer, a PSA and a home monitor.

4. (Previously presented) The system of claim 1 wherein said sensing unit includes at least one of a finger scanner, a camera and a microphone.

5. (Original) The system of claim 4 wherein said biometric traits include a finger scan obtained from said finger scanner.

6. (Previously presented) The system of claim 4 wherein said biometric traits include one of an iris scan and a retina scan obtained via said camera.

7. (Original) The system of claim 4 wherein said biometric traits include a voice print obtained from said microphone.

8. (Currently Amended) A biometric-based user authentication system for identifying and granting access to at least one user to an implanted medical device in a patient associated with an instrument, the authentication system comprising:

at least one biometric sensor implemented in the instrument;

at least one biometric trait of a user stored as coded data in a memory bank of said biometric sensor; and

means for analyzing and comparing said at least one biometric trait with said coded data to grant or deny access, wherein, in response to a potential user being denied access, the analyzing means determines whether the potential user is requesting access associated with an override function and, in response to the access request being associated with the overdrive function, granting a level of access associated with a predetermined authorization level.

9. (Original) The system of claim 8 wherein said at least one biometric sensor includes at least one of a camera, a finger print sensor and a microphone.

10. (Previously presented) The system of claim 8 wherein said at least one biometric trait of a user includes a fingerprint, a voice print, an iris print, a retinal print, a facial model, a veinal imprint and a digital signature.

11. (Original) The system of claim 8 wherein said means for analyzing and comparing includes a software system implemented in the memory bank of the biometric sensor.

12. (Original) The system of claim 8 wherein said biometric traits of a user stored as coded data includes instructions to allow a user with matching biometric traits to have access to a pre-determined set of data and tools of said implanted medical device.

13. (Currently Amended) A method for a biometric-based identification of a user to provide authorized access to operational hardware, software and patient medical data contained in instruments and implanted medical devices, the method comprising:

accepting at least one biometric trait from a potential user;

comparing said at least one biometric trait to a stored coded data;

granting a qualified access when a match is confirmed between said at least one biometric trait and the stored coded data; and

determining, in response to a match not being confirmed between said at least one biometric trait and the stored coded data, whether the potential user is requesting access associated with an override function and, in response to the access request being associated with the overdrive function, granting a level of access associated with a predetermined authorization level.

14. (Original) The method of claim 13 wherein said qualified access includes a hierarchical scheme to enable user-specific access and authorization based on expertise and need.

15. (Original) The method of claim 14 wherein said hierarchical scheme includes distinctions of access to various hardware, software tools to perform therapy, diagnostic and monitoring functions designed to provide various levels of authorized access to physicians, nurses, Medtronic technicians, patients and their representatives.